UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/826,046 | 04/04/2001 | Charles Steven Lingafelt | RSW920010056US1 | 2366 |

26502 7590 08/19/2004

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

| EXAMINER |
|---|
| ZAND, KAMBIZ |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | 4 |

DATE MAILED: 08/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

3

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/826,046 | **Applicant(s)**<br>LINGAFELT ET AL. | |
| | **Examiner**<br>Kambiz Zand | **Art Unit**<br>2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 April 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 April 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *2/04-04-01*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

## DETAILED ACTION

1. **Claims 1-9** have been examined.

### Drawings

2. The drawings filed on 04/04 2001 are accepted by Examiner.

### *Information Disclosure Statement PTO-1449*

3. The Information Disclosure Statement submitted by applicant on 01/09/2003 and 04/04/2001 (paper number 2) has been considered. Please see attached PTO-1449.

### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1-3 and 5-8** are rejected under 35 U.S.C. 102(b) as being anticipated by Coley et al (5,826,014A).

**As per claim 1** Coley et al (5,826,014A) teach a method for improving the operation of equipment used to protect a web server against attack (**see fig.4a where a method to protect a web-server against intruder or an attack is demonstrated by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a**), comprising the acts of: reading a source address of a message received during an attack (**see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a**); checking a database of privileged source addresses (**see fig.2, item 218; col.11, lines 27-30 where the comparison of the source address with the list of "authorized addresses" that corresponds to Applicant's privileged source address being conducted and where "the list of the authorized addresses" that maintains by database 218 of fig.2**); and instructing protective equipment for a web server to pass the received message to the web server when the source address of the received message matches an address contained in the database of privileged source addresses (**see col.11, lines 31-40 where a match between the source address and the address in the authorized list is valid by comparison as shown in step 414 of fig.4a**

**and where after validation connection to the destination in the web server is initiated for sending the message).**

**Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.**

**As per claims 2 and 3** Coley et al (5,826,014A) teach the method of claim 1, wherein the database of privileged source addresses includes a source address of a customer/user known to the web server **(see fig.2, item 200 and fig.3, items 302 or 300 that corresponds to a customer or a user in conjunction with col.11, lines 27-30 their address as a source address in being stored in an authorized list for access request; fig.4b disclose further the authentication procedure of a user or a customer for access).**

**As per claim 5** Coley et al (5,826,014A) teach a Protective equipment for guarding a web server against attack **(see fig.2 where a protective equipment such as item 210 firewall is to protect a web-server against intruder or an attack as described in fig.4a by source address, service and time verification where a failure result in deny access to the web-server; col.5,**

**lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a),** comprising: an address decoder for reading a source address of a message received during an attack (**see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a**); a database of privileged source addresses (**see fig.2, item 218 and col.11, lines 27-30 where the list of the "authorized addresses" that corresponds to "privileged source addresses" and list of unauthorized addresses are maintain in the database of 218 of fig.2**); and logic for instructing protective equipment for a web server to pass the message received during the attack to the web server when the source address of the message received during the attack matches a privileged source address contained in the database of privileged source addresses (**see fig.2, item 18; col.11, lines 27-30 where the comparison of the source address with the list of authorized addresses that corresponds to Applicant's privileged source address being conducted where the list of the authorized addresses that maintain; see col.11, lines 31-40 where a match between the source address and the address in the authorized list is valid by comparison as shown in step 414 of fig.4a then connection to the destination is initiated for sending the message).**

**Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.**

**As per claims 6 and 7** Coley et al (5,826,014A) teach the intrusion detection security system of claim 5, wherein the database of privileged source addresses includes a source address of a customer/user known to access the web server **(see fig.2, item 200 and fig.3, items 302 or 300 that corresponds to a customer or a user in conjunction with col.11, lines 27-30 their address as a source address in being stored in an authorized list for access request; fig.4b disclose further the authentication procedure of a user or a customer for access).**

**As per claim 8** Coley et al (5,826,014A) teach a Protective equipment for guarding a web server against attack (**see fig.4a where a method to protect a web-server against intruder or an attack is demonstrated by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-**

**server of fig.4a)**, comprising: an address decoder for reading a source address of a message received during an attack (**see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a**); a database of privileged source addresses; a database of blocked source addresses (**see fig.2, item 218 and col.11, lines 27-30 where the list of the "authorized addresses" that corresponds to "privileged source addresses" and list of "unauthorized addresses" that corresponds to "blocked addresses" are maintain in the database 218 of fig.2**); and logic for checking the database of privileged source addresses and the database of blocked source addresses for appearance of the source address of the message received during the attack and, responsive to the appearance, instructing protective equipment to block incoming message that bear the source address of the message received during the attack (**see fig.4a, item 412, 414 and 416; col.11, lines 27-33 where the comparison of the source address with the list of authorized addresses that corresponds to Applicant's privileged source address and list of unauthorized addresses that corresponds to block source addresses being conducted and in case of invalidation address it block the access by deny access message**).

**Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the**

**form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.**

## *Claim Rejections - 35 USC § 103*

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 4 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al (5,826,014A) in view of Comey et al (6,363,489 A).

**As per claim 4 Coley et al (5,826,014A)** teach a method for improving the operation of equipment used to protect a web server against attack by a vandal **(see fig.4a where a method to protect a web-server against intruder or an attack is demonstrated by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a**), comprising the acts of:

reading a source address of a message received during an attack (**see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a**); checking a database of privileged source addresses for appearance of the source address of the received message (**see fig.2, item 218; col.11, lines 27-30 where the comparison of the source address with the list of "authorized addresses" that corresponds to Applicant's privileged source address being conducted and where "the list of the authorized addresses" that maintains by database 218 of fig.2**); when the source address of the received message appears in the database of privileged source addresses, instructing protective equipment to pass the received message to a web server (see **col.11, lines 31-40 where a match between the source address and the address in the authorized list is valid by comparison as shown in step 414 of fig.4a and where after validation connection to the destination in the web server  is initiated for sending the message**); when the source address of the received message does not appear in the database of privileged source addresses, checking a database of blocked source addresses for appearance of the source address of the received message; and when the source address of the received message does not appear in the database of blocked source addresses and instructing the protective equipment to block the received message **(see fig.4a, item 412, 414 and 416; col.11, lines 27-33**

**where the comparison of the source address with the list of authorized addresses that corresponds to Applicant's privileged source address and list of unauthorized addresses that corresponds to block source addresses being conducted and in case of invalid source address it block the access by deny access message)** but do not disclose explicitly adding the source address of the received message to the database of blocked source addresses and to block subsequent messages that bear the source address of the received message.

However **Comey et al (6,363,489 A)** teach a method for automatic intrusion detection in a network (see fig.1) having database to store hostile or unauthorized source address (fig.2) that adds the source address of the received message to the database of blocked source addresses **(see col.6, lines 57-60)** and to block subsequent messages that bear the source address of the received message **(see col.6, lines 61-64). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize** Comey's adding of unauthorized source addresses in Coley's list of unauthorized source addresses in the database and blocking the subsequent messages from the blocked addresses into the network of Coley's in order to contain these messages in a secure zone by diverting or redirecting messages in order to blocking the unauthorized user from such attempt at access.

**As per claim 9** Coley et al (5,826,014A) teach a Protective equipment for guarding a web server against attack (**see fig.4a where a method to protect a**

**web-server against intruder or an attack is demonstrated by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a**), comprising: an address decoder for reading a source address of a message received during an attack (**see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a**); a database of privileged source addresses; a database of blocked source addresses (**see fig.2, item 218 and col.11, lines 27-30 where the list of the "authorized addresses" that corresponds to "privileged source addresses" and list of "unauthorized addresses" that corresponds to "blocked addresses" are maintain in the database 218 of fig.2**); and logic for checking the database of privileged source addresses for appearance of the source address of the received message; when the source address of the received message appears in the database of privileged source addresses, instructing protective equipment to pass the received message to a web server (**see col.11, lines 31-40 where a match between the source address and the address in the authorized list is valid by comparison as shown in step 414 of fig.4a and where after validation connection to the destination in the web server is initiated for sending the message**); when the source address of the received message does not appear in the database of privileged source addresses, checking the database of blocked source addresses for appearance of the source address of the received message; and When the source address of the received message does not appear in the database of blocked source addresses and instructing the protective equipment to block the received message **(see fig.4a, item 412, 414 and 416; col.11, lines 27-33 where the comparison of the source address with the list of authorized addresses that corresponds to Applicant's privileged source address and list of unauthorized addresses that corresponds to block source addresses being conducted and in case of invalid source address it block the access by deny access message). Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.**

Coley et al (5,826,014A) however do not explicitly disclose adding the source address of the received message to the database of blocked source addresses and to block subsequent messages that bear the source address of the received message.

However **Comey et al (6,363,489 A)** teach a method for automatic intrusion detection in a network (see fig.1) having database to store hostile or unauthorized source address (fig.2) that adds the source address of the received message to the database of blocked source addresses **(see col.6, lines 57-60)** and to block subsequent messages that bear the source address of the received message **(see col.6, lines 61-64). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize** Comey's adding of unauthorized source addresses in Coley's list of unauthorized source addresses in the database and blocking the subsequent messages from the blocked addresses into the network of Coley's in order to contain these messages in a secure zone by diverting or redirecting messages in order to blocking the unauthorized user from such attempt at access.

## Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S.Patent No. US (6,615,358 B1) teach firewall for processing connection-oriented and connection-less datagram over a connection-oriented network.

U.S.Patent No. US (6,052,788 A) teach firewall providing enhanced network security and user transparency.

U.S.Patent No. US (6,735,702 B1 ) teach method and system for diagnosing network intrusion.

U.S.Patent No. US (5,884,025 A) teach system for packet filtering of data packet at a computer network interface.

U.S.Patent No. US (6,598,167 B2 ) teach secure customer interface for WEB data management.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

08/12/04